Page 11342

b. When Privacy and Security Certification Criteria Apply to EHR Modules:

We believe that EHR Modules hold great promise with respect to innovation. However, we also recognize that the potential innovative benefits EHR Modules can provide will be significantly compromised if these same EHR Modules do not include appropriate privacy and security safeguards to instill trust. EHR Modules can come in many forms and can provide a large set of capabilities or a single capability. This variability, which promotes innovation, also poses several challenges to determining when it is appropriate to require EHR Modules be tested and certified to the privacy and security certification criteria adopted by the Secretary (45 CFR 170.302(o) through
(v)).

Our goal for determining when this should occur is two-fold: (1) Assure eligible professionals and eligible hospitals that EHR Modules will not negatively affect how Certified EHR Technology in its entirety protects electronic health information; and (2) appropriately require (or not require) the testing and certification of EHR Modules to privacy and security certification criteria.

In the context of EHR Modules and testing and certification, it is important to keep in mind that we are discussing a point before ''implementation'' in the HIT lifecycle. Accordingly, ONC–ATCBs will test and certify EHR Modules independent of, and disassociated from, their potential operating environments.

Below, we identify several challenges to determining when an ONC–ATCB should be required to test and certify EHR Modules to the privacy and security certification criteria adopted by the Secretary. After discussing these challenges, we propose, and request public comment on, a potential approach that establishes when ONC–ATCBs should be required to test and certify EHR Modules to the privacy and security certification criteria adopted by the Secretary in addition to the capability or capabilities the EHR Module may be specifically designed to provide.

One challenge with respect to determining when EHR Modules should be tested and certified to the privacy and security certification criteria adopted by the Secretary occurs when EHR Modules operate in an environment separate from other HER Modules—when they are so-to-speak ''autonomous.'' For example, an e-prescribing EHR Module or a patient portal EHR Module provided by an application service provider (ASP) could be hosted and maintained by the ASP (not by the end-user). In these cases, an end-user (*e.g.,* eligible professional) may be unable to control or specify the level or amount of privacy and security safeguards associated with the health information stored, modified, or transmitted by the EHR Module.

We believe that it would be irresponsible and potentially dangerous to permit such EHR Modules to be tested and certified solely to their specific capability, and not to the privacy and security certification criteria adopted by the Secretary. On the flipside, a second challenge relates to EHR Modules that, by design, may provide specific capabilities which make it technically infeasible to require that they separately meet the privacy and security certification criteria adopted by the Secretary. One example could be a medication reconciliation EHR Module which, from a technical perspective, would be designed to function ''behind the scenes'' as part of the internal workings of Certified EHR Technology. In all likelihood, it would therefore depend on another EHR Module's or EHR Modules' privacy and security capabilities. In this example, we believe that it would be technically infeasible for the medication reconciliation EHR Module to have its own authentication capability because, in all likelihood, an end-user would have had to have been authenticated prior to gaining access to the medication reconciliation EHR Module. Conversely, while it is unlikely that the medication reconciliation EHR Module would retain or store health information, other EHR Modules might, and it may be appropriate to require such EHR Modules to be tested and certified to some or all of the privacy and security certification criteria adopted by the Secretary.

Because of the context specific nature of EHR Modules, and the fact that we expect them to provide any different capabilities, it is difficult to establish with absolute certainty an approach that will work for all EHR Modules. However, we believe that an appropriate starting point for such an approach should focus first on protecting individuals' health information and then on whether there exist appropriate exceptions to the approach that would exempt EHR Modules from the requirement to be tested and certified to adopted privacy and security certification criteria. As a result, we propose that ONC–ATCBs would be required to test and certify all EHR Modules to the privacy and security certification criteria adopted by the Secretary unless the EHR Modules is/are presented for testing and certification in one of the following manners:

• The EHR Module(s) are presented for testing and certification as a precoordinated, integrated ''bundle'' of EHR Modules, which could otherwise constitute a Complete EHR. In such instances, the EHR Module(s) would be tested and certified in the same manner as a Complete EHR. Because the bundle of EHR Modules would constitute a single, integrated product, we believe that it would be unnecessary in such cases to require each EHR Module to be tested and certified independently to privacy and security certification criteria. We propose one variation to this exception for pre-coordinated bundles of EHR Modules which include EHR Module(s) that would not be part of an eligible professional or eligible hospital's local system and under its direct control (*e.g.,* a patient portal EHR Module that is not hosted and maintained). In these situations, the constituent EHR Modules of such an integrated bundle would need to be separately tested and certified to all privacy and security certification criteria;

• An EHR Module is presented for testing and certification, and the presenter can demonstrate to the ONC–ATCB that it would be technically infeasible for the EHR Module to be tested and certified in accordance with some or all of the privacy and security certification criteria. For example, we believe that it would be technically infeasible for an EHR Module that does not store even temporarily, or maintain any health information to be required to include a capability to encrypt health information at rest or include an audit log. Alternatively, it would presumably be technically infeasible for an EHR Module that does not provide a capability for exchange to be required to include the capabilities to encrypt health information for exchange or account for treatment, payment, or health care operations disclosures; or

• An EHR Module is presented for testing and certification, and the presenter can demonstrate to the ONC– ATCB that the EHR Module is designed to perform a specific privacy and security capability. In such instances, we do not believe that it should be tested and certified to the other privacy and security certification criteria adopted by the Secretary. For example, an encryption EHR Module would *not* be required to be tested and certified as also including the capability to terminate an electronic session after a predetermined time of inactivity. We believe that the approach we have articulated above provides an appropriate framework for determining when ONC–ATCBs would be required to test and certify EHR Modules to the privacy and security certification criteria adopted by the Secretary.

We request public comment on whether there are additional alternatives to the ones proposed above and other circumstances where an EHR Module should be tested and certified to none, some, or all of the privacy and security certification criterion adopted by the Secretary.